, join our discord if you haven't already!

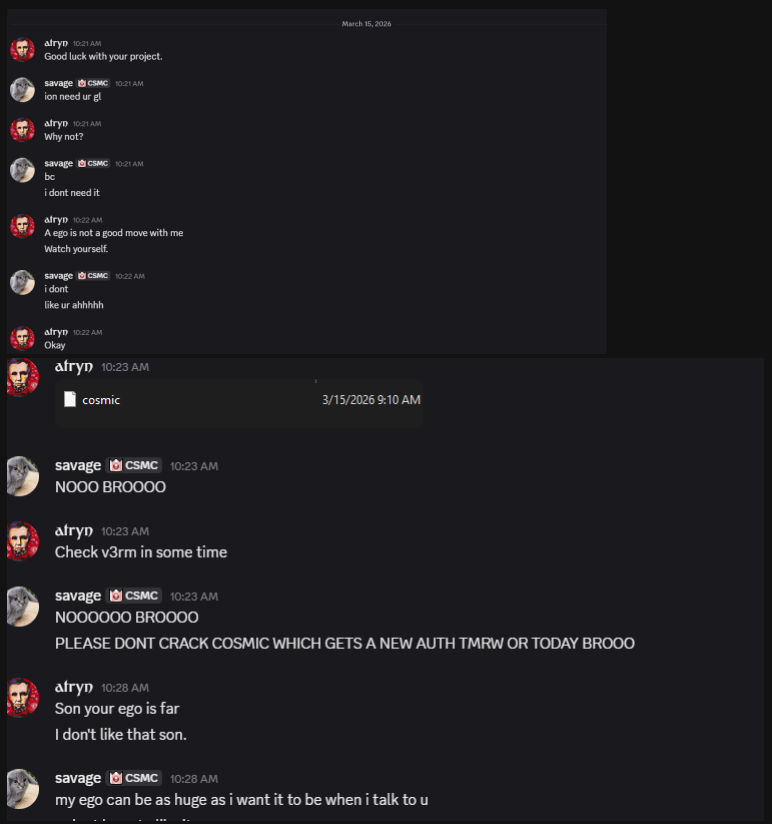
[RELEASE] Cosmic, Isaeva, Wave, Velocity Injector

atryn · 50 minutes ago · 23 · 270

A
atryn
Member
Reputation: 0

50 minutes ago New #1

I've been out of the community for a long time, but I recently saw a new exploit released by Savage. As you know, I don't really mind cheats but Savage has a huge ego. I tried wishing him good luck, and he told me to go fuck myself.



Little did he know.. this was more then a crack.

So instead of bothering to crack the cheat, I'll do something far more effective and let the Hyperion team deal with it.

I'm not going to leak the full injection method, but I will explain how it's made.

The injection method used here is the same one utilized by Wave, Velocity, Isaeva, and now Cosmic.

This is not the exact dll these tools utilize but one that is the exact same I found.

You can use **pots.dll** . Make a function that loads a real Windows DLL into Roblox. Hyperion will automatically whitelist this DLL. You MUST ensure your DLL is smaller than or equal to the shell DLL. If pots.dll is 100KB, your DLL cannot be 101KB. If it is larger, you have to split your code into multiple caves.

Once the shell is loaded, we overwrite its "guts" with our own DLL code.

0. Syscalls and why you need to use it for this injector

Normally, when you call WriteProcessMemory, you are calling code inside kernel32.dll, which then calls ntdll.dll. Hyperion "hooks" these functions. They place a "JUMP" at the start of the function that sends your data to them for inspection before it ever reaches the Kernel. **Syscalls** allow you to skip the middleman. You talk directly to the CPU and say: "Hey Kernel, do this for me," completely jumping over the hooked functions in ntdll.dll.

If you just put a syscall instruction in your own code, Hyperion will catch you instantly. Why? Because legitimate programs **never** have raw syscall instructions; they always use the ones inside ntdll.dll.

injectors use **Indirect Syscalls**:

1. They find a real syscall instruction inside a signed Windows file (like ntdll.dll).
2. They set up the registers (RCX, RDX, etc.).
3. They "Jump" to that real syscall instruction.
4. To the CPU, it looks like a legitimate Windows function made the request.

Windows has a feature called **ProcessInstrumentationCallback**. Hyperion sets this up so that every time a syscall finishes, the CPU jumps to Hyperion's code first before returning to the injector. Hyperion then looks at the Return Address on the stack. If that address points to a "Code Cave" or "Stomped Module," you are flagged.

When a syscall is made, Hyperion can inspect the **Call Stack**.

- **Legit Call**: App.exe -> User32.dll -> Ntdll.dll -> Kernel.
- **Cheater Call**: StompedModule.dll -> Kernel. Hyperion sees the "missing links" in the stack and knows the request didn't come from a legitimate program.

The Only Way Out

This is why **Module Stomping** is required. By stomping a real DLL, your "Return Address" and "Stack Frame" look like they belong to a real, authorized Windows component.

1. Copying Sections

We don't just copy the whole file. We copy each part (header, text, data) to its specific place.

Code:

```
void copy_sections(void* process_handle, void* target_base, void* src_data) {
    auto* nt = get_nt_header(src_data);
    auto* section = get_first_section(nt);

    for (int i = 0; i < nt->file_header.number_of_sections; i++) {
        void* dest = (unsigned char*)target_base + section[i].virtual_address;
        void* src = (unsigned char*)src_data + section[i].pointer_to_raw_data;
        write_process_memory(process_handle, dest, src, section[i].size_of_raw_data);
    }
}
```

2. Fixing Relocations (Base Delta)

Our code expects to be at one address, but the shell DLL is at another. We fix this by adding the "Delta" (difference) to every hardcoded address in the code.

C++:

```
void fix_relocations(void* base, unsigned long_ptr delta) {
    auto* reloc_dir = get_reloc_directory(base);
    auto* reloc_data = (image_base_relocation*)((unsigned char*)base + reloc_dir->virtual_address);

    while (reloc_data->size_of_block) {
        int entries = (reloc_data->size_of_block - sizeof(image_base_relocation)) / sizeof(unsigned short);
        unsigned short* info = (unsigned short*)(reloc_data + 1);

        for (int i = 0; i < entries; i++) {
            if ((info[i] >> 12) == 10) { // IMAGE_REL_BASED_DIR64
                unsigned long_ptr* patch = (unsigned long_ptr*)((unsigned char*)base + reloc_data->virtual_address + (info[i] & 0xFFF));
                *patch += delta;
            }
        }
        reloc_data = (image_base_relocation*)((unsigned char*)reloc_data + reloc_data->size_of_block);
    }
}
```

2. Resolving Imports

This is up to you, this is a one line matter so I won't feed it.

3. Injection

The injector finds an existing handle to the Thread Pool's "I/O Completion Port" inside Roblox. It uses DuplicateHandle to get its own copy of that handle.

We create a structure called TP_DIRECT. We set its "Callback" to the address of our shellcode.

C++:

```
void prepare_trigger(void* shellcode_addr) {
    struct tp_direct {
        void* callback;
        // other fields
    };

    tp_direct work;
    work.callback = shellcode_addr;
}
```

Use poolparty for this.

Code:

```
void trigger_execution(void* hijacked_io_port, void* remote_work_item) {
    zw_set_io_completion(hijacked_io_port, remote_work_item, 0, 0, 0);
}
```

The code runs inside a real thread. By using a hijacked handle, the injector doesn't have to open anything. Meaning Hyperion does not see this.

Summary for Skids

1. Module Stomping: You are "wearing a costume" of a real Windows DLL.
2. Poolparty: You are "hitchhiking" on a real game thread instead of making your own.
Because you are inside a "Safe" memory region and running on a "Safe" thread, you are invisible.

Hyperion will patch this soon as they will add integrity scanning for these regions, as of now there is none.

Files leaked

Gofile - Cloud Storage Made Simple
Secure, fast and free cloud storage solution. Upload and share files instantly.
gofile.io

VirusTotal
VirusTotal
www.virustotal.com

VirusTotal
VirusTotal
www.virustotal.com

WARNING THESE ARE SKIDDED..

Savage, oh boy you tuff ash.

C++:

```
local Signal = {}
Signal.__index = Signal

function Signal.new()
    local self = {
        _connections = {},
        _onceConnections = {},
        _waitingThreads = {},
        _nextId = 1
    }
    return setmetatable(self, Signal)
end

function Signal:Connect(handler)
    assert(type(handler) == "function", "Signal:Connect expected function, got " .. type(handler))

    local id = self._nextId
    self._nextId += 1

    local connection = {
        Id = id,
        Function = handler,
        Connected = true,
        Signal = self
    }

    self._connections[id] = connection

    local connectionObj = {
        Connected = true,
        Disconnect = function()
            if connection.Connected then
                connection.Connected = false
                self._connections[id] = nil
            end
        end
    }
```

6 AM

You were banned in Cosmic. | mad bc pearl was shit

Proceeds to use LUA signals?!!!!!!!

NO wonder why this is $10 lifetime.

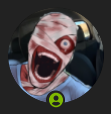
```
<!DOCTYPE html>
<!-- saved from url=(0023)http://tauri.localhost/ -->
<html lang="en" style="--k-bg: #0d0f1a; --k-surface: #151829; --k-su
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=
        <link rel="icon" type="image/svg+xml" href="http://tauri.loc
        <meta name="viewport" content="width=device-width, initial-s
        <link rel="preconnect" href="https://fonts.googleapis.com/">
        <link rel="preconnect" href="https://fonts.gstatic.com/" cro
        <title>SavajLaxazpSploit</title>
        <style>
            /* Prevent white flash on load */
            html, body, #root {
                background-color: #0d0f1a;
                margin: 0;
                padding: 0;
                width: 100%;
                height: 100%;
                overflow: hidden;
            }

            /* Custom scrollbar (apply to document for WebView) */
            * {
                scrollbar-width: thin;
                scrollbar-color: #444 transparent;
            }

            ::-webkit-scrollbar {
                width: 6px !important;
                height: 6px !important;
            }

            ::-webkit-scrollbar-track {
                background: transparent !important;
            }

            ::-webkit-scrollbar-thumb {
                background: #444 !important;
```

I love the AI!

Last edited: 20 minutes ago

Report

Like Reply

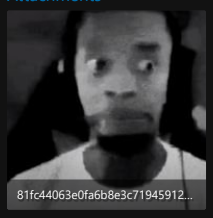


olemadiosum
Active Member
Reputation: 4

47 minutes ago New #2

thx making Olemad Sploit Right now

Attachments

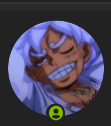


Staff Lead @ Swift
Staff Lead @ Bunni
https://www.youtube.com/@Olemad

Report

Like Reply

hotdog14156v2 and Steel



lilblackie
Active Member
Reputation: 0

45 minutes ago New #3

> olemadiosum said:
> thx making Olemad Sploit Right now

ud bro

Hating has no limits. - A Random v3rm user

Report

Like Reply

N

notphilip510
Active Member
Reputation: 0

44 minutes ago New #4

We would have preferred a crack. Fuck you for ruining exploits.

Report

Like Reply

A

atryn
Member
Reputation: 0

43 minutes ago New #5

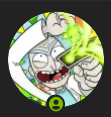
> notphilip510 said:
> We would have preferred a crack. Fuck you for ruining exploits.

No point.. A new authentication system is coming in. I'll crack it once it drops.

For now, enjoy Cosmic getting patched.

Report

Like Reply



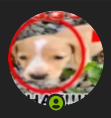
henrickiscool
Newbie
Reputation: 0

40 minutes ago New #6

thx +rep working on win vista

Report

Like Reply



iretq
Active Member
Reputation: 0

38 minutes ago New #7

dyn/tux/wtv you completely missed the point, you are using old and outdated information about hyperion and thinking hyperion works on all processes and what you said is just basic open source mmap with basic open source threadpool execution and the dll overwriting part is also wrong

Report

Like Reply

kee, olemadiosum and makesurecrackacums

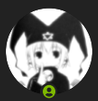
0100111101110011011
Member
Reputation: 0

37 minutes ago New #8

how do i use ts

Report

Like Reply

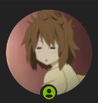


csaxxx
Newbie
Reputation: 0

36 minutes ago New #9

w making vonsploit rn

Report Like Reply



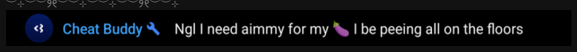
Steel
Active Member
Reputation: 0

36 minutes ago New #10

> olemadiosum said:
>
> thx making Olemad Sploit Right now

omg we are ALL spending 1000$ on olesploit UD 10million sunc

⁀⊹⁀⁀୨ɛ⁀⁀⊹⁀⁀⊹⁀⁀୨ɛ⁀⁀⊹
she/her
ᶜᵃᵛᵉʳⁿⁱˢᵗᵘᶠᶠ.ᶜᶜ (my site)
ᵒᵇʳˢʷᵃʳᵉ.ˢᵗᵒʳᵉ (buy from here)
⁀⊹⁀⁀୨ɛ⁀⁀⊹⁀⁀⊹⁀⁀୨ɛ⁀⁀⊹



Report Like Reply

A

atryn
Member
Reputation: 0

36 minutes ago New #11

> iretq said:
>
> dyn/tux/wtv you completely missed the point, you are using old and outdated information about hyperion and thinking hyperion works on all processes and what you said is just basic open source mmap with basic open source threadpool execution and the dll overwriting part is also wrong

Wrong, Wrong, Wrong. THis method still works. No one said "on all processes". This DLL specifically works. You can use threadpool and it works fine. The overwriting part is completely correct. Don't defend a pedophile please.

Report Like Reply

arg
Active Member
Reputation: 0

34 minutes ago New #12

Buy my new exploit.

Report Like Reply

C

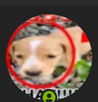
CozzyCCH
Active Member
Reputation: 0

34 minutes ago New #13

> iretq said:
>
> dyn/tux/wtv you completely missed the point, you are using old and outdated information about hyperion and thinking hyperion works on all processes and what you said is just basic open source mmap with basic open source threadpool execution and the dll overwriting part is also wrong

i didnt do ts get off my dick brother

Report Like Reply



iretq
Active Member
Reputation: 0

34 minutes ago New #14

> CozzyCCH said:
>
> i didnt do ts get off my dick brother

ok mr riot client

Report Like Reply

C

CozzyCCH
Active Member
Reputation: 0

33 minutes ago New #15

> iretq said:
>
> ok mr riot client

ok mr leaked his email on screenshare

Report Like Reply

azul
Active Member
Reputation: 0

29 minutes ago New #16

> 0100111101110011011 said:
>
> how do i use ts

cooked

Report Like Reply

29 minutes ago New #17

60% of info wrong nice post ig

int is 8 bytes... - Fagnar ChocoSploit Owner&Developer...

Report Like Reply

makesurecrackacums
Active Member
Reputation: 3

28 minutes ago New #18

> makesurecrackacums said:
> 60% of info wrong nice post ig

Are we sure? I have a GC right now everyone saying it's right and they have a injector with it.

All I wanted was to be cool, you made the wrong move. Hatred for what?

Report Like Reply

atryn
Member
Reputation: 0

21 minutes ago New #19

> atryn said:
> Are we sure? I have a GC right now everyone saying it's right and they have a injector with it.
>
> All I wanted was to be cool, you made the wrong move. Hatred for what?

im sure zaar

int is 8 bytes... - Fagnar ChocoSploit Owner&Developer...

Report Like Reply

makesurecrackacums
Active Member
Reputation: 3

16 minutes ago New #20

50% sure seraphim uses this method to as xrc and cg where laughing about indirect syscalls in vc

> atryn said:
> Are we sure? I have a GC right now everyone saying it's right and they have a injector with it.
>
> All I wanted was to be cool, you made the wrong move. Hatred for what?

Report Like Reply

azul
Active Member
Reputation: 0

1 2 Next ›

Preview

Write your reply...

Attach files Post reply

Similar threads

[RELEASE] Warfare silent aim + walkspeed egwergtq5123 · Jan 30, 2026 · Roblox	Replies: 3 Views: 239	Feb 14, 2026 egwergtq5123
abyys again bypass spanksterria · Feb 12, 2026 · Roblox	Replies: 3 Views: 182	Feb 12, 2026 poptartlover
you vs homer anti cheat bypass [real one that doesnt break games this time lmfao] getpcd · Mar 3, 2026 · Roblox	Replies: 11 Views: 262	Mar 4, 2026 zins
[open source] fast blade ball parry function nathan bjork · Jan 1, 2026 · Roblox 2 3	Replies: 42 Views: 1K	Feb 7, 2026 foidgee
is there any way to prevent abusive usage of the script global by game devs nathan bjork · Jul 24, 2025 · Roblox 2	Replies: 23 Views: 540	Jul 26, 2025 nathan bjork

Share:

Exploiting › Roblox ›

Community platform by XenForo® © 2010-2025 XenForo Ltd.
Quality Add-Ons made with by WMTech © 2026 WebMachine Technologies, Inc.
ok